RFID et sécurité font-elles bon ménage ?

Gildas Avoine

Massachusetts Institute of Technology
Cambridge, MA 02139, USA

Résumé Alors que l'identification par radiofréquence (RFID) est devenue une technologie incontournable, de nombreuses questions se posent, tant au sujet de la sécurité que cette technologie apporte, qu'au sujet des risques liés à la vie privée qu'elle fait encourir. Cet article offre une introduction à la RFID et décrit les problèmes de sécurité auxquels cette technologie est confrontée, en présentant quelques exemples. En particulier, plusieurs attaques sur des systèmes de contrôle d'accès sont exposées.

1 Introduction

L'identification par radiofréquence (RFID) fait aujourd'hui couler beaucoup d'encre. Cette technologie qui permet d'identifier à distance des objets sans contact physique ni visuel est relativement simple à mettre en œuvre. Elle nécessite des transpondeurs, appelés *tags* ou parfois *étiquettes* qui sont apposés sur les objets à identifier ; des lecteurs qui permettent d'interroger ces tags par radiofréquence ; et un système de traitement de données, qui peut être centralisé ou distribué dans chaque lecteur. Déjà existante durant la seconde guerre mondiale, cette technologie est loin d'être nouvelle. Cependant, la RFID que l'on connaît aujourd'hui n'a plus grand chose à voir avec son ancêtre, qui permettait à la RAF de distinguer les avions alliés des avions ennemis. Bien sûr, les principes électromagnétiques sur lesquels elle repose restent les mêmes, mais les progrès réalisés en électronique ont radicalement changé la donne : le prix d'un tag peut atteindre une quinzaine de centimes d'euros et sa taille est parfois inférieure à un grain de riz.

Parce qu'il existe de nombreuses applications différentes qui peuvent tirer profit de la RFID, il existe tout un panel de tags. Ceux-ci peuvent se caractériser par leur prix, leur taille, leur capacité de calcul ou de stockage, leur distance de communication, ou tout autre critère plus ou moins corrélé aux précédents. Il n'existe cependant pas beaucoup de points communs entre un tag à 15 centimes d'euros (qui ne contient qu'une simple mémoire d'une centaine de bits) et un tag à plusieurs euros (qui peut éventuellement posséder sa propre source d'énergie, contenir plusieurs kilo-bits de mémoire ré-inscriptible et effectuer des calculs cryptographiques).

Le standard EPG Global de deuxième génération [6] distingue quatre classes de tags. La *classe 1* correspond aux tags les moins performants et donc les moins chers. Ils sont dotés d'une mémoire accessible en lecture seulement, qui contient

un identifiant unique (typiquement 128 bits). Lorsque le tag est interrogé par un lecteur, il envoie simplement son identifiant. Les tags de classe 1 se trouvent dans les bibliothèques, les chaînes logistiques, etc. La *classe 2* permet d'implémenter des fonctions sur le tag, typiquement un algorithme cryptographique symétrique et de posséder quelques centaines de bits de mémoire ré-inscriptible. Cependant, les tags des classes 1 et 2 sont *passifs* c'est-à-dire qu'il ne possèdent pas de batterie et doivent donc être présents dans le champ du lecteur pour communiquer et effectuer des calculs. Ces tags ont une distance de communication relativement faible : quelques décimètres en haute fréquence et jusqu'à quelques mètres en ultra-haute fréquence. On considère enfin que leur résistance aux attaques physiques est très limitée : on admet généralement qu'une même information secrète ne doit pas être partagée par plusieurs tags pour limiter les conséquences d'une telle attaque. Les tags de *classe 3* sont semi-passifs, c'est-à-dire qu'ils possèdent une source d'énergie interne pour réaliser des calculs, mais l'énergie apportée par le lecteur est toujours nécessaire pour la communication. Enfin, les tags de *classe 4* sont *actifs*, possédant une batterie utilisée à la fois pour les calculs et la communication, ce qui leur permet d'initier eux-mêmes des échanges avec un lecteur et de posséder une distance de communication plus importante. Le standard [6] considère également que les tags de classe 4 peuvent communiquer entre eux.

L'engouement que connaît la RFID depuis quelques années concerne les tags de classe 1 et de classe 2. Nous nous concentrerons sur ces tags dans la suite.

Outre la classification des tags, il est essentiel de classer les applications en fonction de leur objectif. Un protocole pour identifier des objets dans une chaîne logistique n'aura en effet pas les mêmes besoins qu'un protocole de contrôle d'accès. On distingue ainsi deux grandes catégories d'applications [2] : celles dont l'objectif est uniquement d'apporter des fonctionnalités nouvelles ou d'améliorer des fonctionnalités existantes (tri sélectif de déchets, remplacement des codes-barres, tatouage du bétail, etc.) et celles dont l'objectif est d'apporter de la sécurité (badge d'accès à un immeuble, clef de démarrage d'une voiture, abonnement aux transports publics, etc.). Dans le premier cas, le but du protocole est d'obtenir l'identité de l'objet interrogé mais aucune preuve de cette identité n'est requise : c'est un *protocole d'identification*. Ce type de protocole est *a priori* suffisant pour la majorité des applications. Il est par exemple suffisant lorsque la RFID est utilisée pour identifier des objets dans une chaîne logistique, en remplacement des codes-barres. Dans le second cas, il est important qu'une *preuve* de l'identité soit fournie : c'est un *protocole d'authentification*. Par abus de langage, *protocole RFID* désigne aussi bien un protocole d'identification qu'un protocole d'authentification. Notons que s'il ne semble pas y avoir de problème de sécurité au sens strict dans le cas du protocole d'identification, en revanche, celui-ci est, comme le protocole d'authentification, sujet aux problèmes liés à la vie privée.

L'objectif de cet article est de donner un aperçu des principaux problèmes de sécurité en RFID. Ainsi, la section 2 rappelle le principe d'un protocole d'authentification et présente quelques systèmes d'authentification qui ont été mal

conçus. La section 3 s'intéresse quant à elle au problème du respect de la vie privée. Enfin, la section 4 conclut cet article en présentant d'autres problèmes de sécurité, encore peu étudiés dans le cadre de la RFID.

2 Contrôle d'accès utilisant des tags RFID

La RFID à bas coût ne peut pas bénéficier de cryptographie à clef publique et doit donc reposer sur la cryptographie symétrique. Le schéma communément utilisé pour réaliser de l'authentification est dit *par question/réponse* : le lecteur envoie un challenge[1] au tag qui prouve son identité en répondant à ce challenge. Évidemment, un adversaire ne doit pas être capable de répondre à la place du tag, même s'il a écouté les précédentes réponses de ce dernier. Pour cela, le lecteur et le tag possèdent un secret k en commun – une clef cryptographique – qui est nécessaire pour calculer la réponse et pour la vérifier. Quant au challenge, il ne doit être utilisé qu'une seule fois (en pratique, la probabilité qu'un challenge soit utilisé plusieurs fois doit être négligeable). D'un point de vue cryptographique, le challenge est une valeur choisie aléatoirement et uniformément dans un espace suffisamment grand. La clef cryptographique doit être choisie de la même manière. En fait, elle doit être suffisamment longue pour éviter toute attaque par recherche exhaustive. Il est communément admis qu'une clef cryptographique symétrique doit comporter au moins 128 bits pour atteindre une sécurité satisfaisante. Répondre au lecteur consiste à chiffrer la valeur aléatoire reçue avec la clef cryptographique, en utilisant un algorithme de chiffrement E. Ce principe est illustré sur la figure 1. L'algorithme de chiffrement est indépendant du proto-

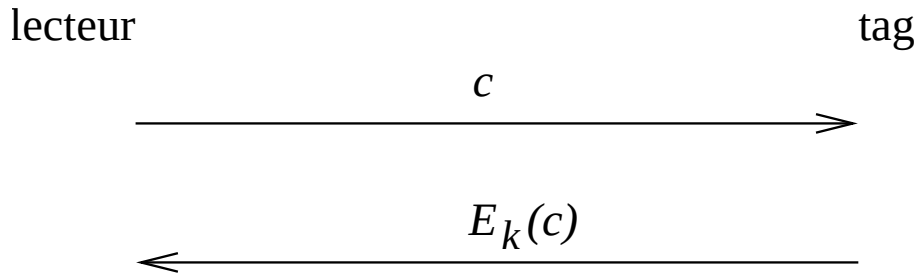

Fig. 1. Protocole par question/réponse

cole lui-même. Cet algorithme doit cependant être sûr (en particulier un pirate ne doit pas pouvoir calculer $E_k(c)$ sans posséder k), ce qui incite à l'utilisation d'algorithmes reconnus, par exemple AES. Si l'algorithme de chiffrement est sûr et s'il est bien utilisé (génération de la clef et du challenge), alors le protocole d'authentification est également sûr.

[1] Le terme anglais *challenge* est généralement utilisé pour désigner la question.

Tous les éléments nécessaires pour constituer un protocole de contrôle d'accès sûr reposant sur la RFID sont donc réunis. Toutefois, nous allons voir dans la suite quelques exemples de systèmes dont la sécurité n'est pas satisfaisante.

2.1 Clefs de démarrage

De nombreuses clefs de voitures intègrent un dispositif RFID relié au système d'injection de carburant. Lorsque la clef est insérée dans le dispositif de démarrage, le tag reçoit un challenge et doit y répondre correctement pour permettre l'activation de l'injection et donc le démarrage du véhicule.

Des chercheurs américains de l'université Johns Hopkins (Maryland) et des laboratoires RSA (Massachusetts) [4] se sont intéressés au module DST (*Digital Signature Transponder*) de Texas Instrument, qui équipe entre autres certains véhicules du constructeur Ford. Après une phase de reverse-engineering (car l'algorithme cryptographique utilisé est propriétaire et non public), ils ont découvert que les clefs utilisées dans les modules DST n'ont une longueur que de 40 bits ! La taille du challenge est également de 40 bits et la réponse est tronquée à 24 bits. En pratique, cela permet à un pirate de découvrir la clef cryptographique contenue dans un module DST à partir de réponses[2] du tag puis en pratiquant une recherche exhaustive sur l'ensemble des clefs. Effectuer une telle recherche exhaustive demande moins d'une heure de calcul, en utilisant un système constitué de 16 FPGA. Étant donné que le pirate peut lui-même choisir son challenge, il peut utiliser un compromis temps-mémoire pour réduire le temps de craquage [8,13]. Dès que les tables ont été pré-calculées, l'attaque nécessite moins d'une minute sur un simple PC et seulement quelques secondes avec le système FPGA mentionné. Notons que si le tag incorporait de l'aléa dans sa réponse, le compromis temps-mémoire ne permettrait plus d'améliorer le temps de craquage.

La distance de communication du module DST est faible, mais s'asseoir à côté de sa victime durant une fraction de seconde est suffisant pour recueillir les informations nécessaire à la reproduction du tag. Le fait qu'un tag réponde au lecteur automatiquement sans demander l'avis du porteur du tag est également problématique car l'attaque peut être menée sans que la victime ne s'en aperçoive.

Notons enfin que la sécurité de la carte de paiement américaine ExxonMobil Speedpass repose aussi sur le dispositif de Texas Instrument. Les chercheurs américains ont donc également démontré la faiblesse de cette carte en effectuant un achat de carburant dans une station essence en simulant leur propre carte avec un ordinateur portable.

La faiblesse du module DST provient du fait qu'un algorithme cryptographique inadapté est consciemment utilisé, probablement afin de réduire le coût du dispositif. Cette pratique est loin d'être isolée et il existe sur le marché de nombreux tags destinés au contrôle d'accès qui possèdent des clefs de 48 bits.

[2] Étant donné que la réponse est tronquée, au moins deux réponses sont en fait nécessaires pour que le pirate soit certain d'avoir trouvé la bonne clef.

2.2 Carte d'identification du MIT

L'arrivée de nouvelles cartes d'identification au *Massachusetts Institute of Technology* (MIT) est aujourd'hui monnaie courante. Depuis 1993, cette université cherche en vain le système qui alliera respect de la vie privée, sécurité et facilité d'utilisation, satisfaisant ainsi tous les utilisateurs. Les cartes actuelles, qui contiennent un tag RFID, sont en service depuis presque trois ans, un record ! Rien ne laissait pourtant présager une telle longévité, car ce système a inquiété dès sa mise en service. Rien d'étonnant lorsque l'on sait que le premier bâtiment équipé de cette nouveauté pour le contrôle d'accès ne fut autre que le fameux building 32, qui compte parmi ses scientifiques le non moins fameux Richard Stallman, fervent défenseur des libertés individuelles, mais aussi toute une panoplie de chercheurs dont la seule raison de vivre est la sécurité et la cryptographie.

L'annonce, en janvier 2004, que les logs des lecteurs étaient conservés à l'insu du personnel a provoqué de nombreuses réactions. Cinq étudiants, P. Agrawal, N. Bhargava, C. Chandrasekhar, A. Dahya et J.D. Zamfirescu [1], ont alors décidé d'étudier le système.

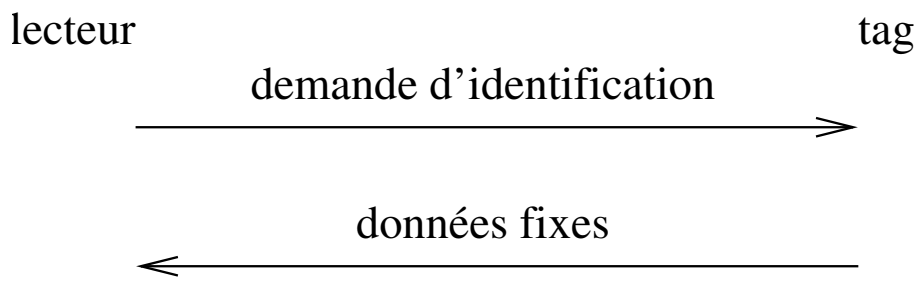

Fig. 2. Protocole utilisé par la carte du MIT

La figure 2 décrit le protocole entre le lecteur et le tag : il ne repose pas sur un schéma de type question/réponse ! Le tag est donc utilisé comme une simple mémoire contenant une valeur fixe qui est retournée au lecteur à chaque nouvelle authentification. Simuler la carte est alors un jeu d'enfant puisqu'il suffit d'écouter la communication entre un lecteur et la carte (une fois suffit) ou, plus simplement, interroger soit-même la carte avec son propre lecteur, pour ensuite pouvoir simuler la carte à volonté, en *rejouant* les données fixes volées. Autrement dit, la carte d'identification du MIT n'apporte pas plus de sécurité qu'un bon vieux *Sésame ouvre toi*.

2.3 Attaques par relais

Les deux exemples de systèmes d'identification décrits précédemment présentaient des faiblesses. Le premier cas (section 2.1) était dû à un mauvais algorithme de chiffrement alors que le second (section 2.2) était dû à l'utilisation

d'un protocole d'identification en lieu et place d'un protocole d'authentification. Lorsqu'un protocole par question/réponse est bien utilisé et qu'il utilise un algorithme de chiffrement reconnu, alors les problèmes précédents ne se produisent pas. Cela ne signifie pas pour autant que tout problème est exclus. En effet, le fait que le tag puisse répondre au lecteur sans l'accord de son possesseur ouvre la voie à un autre type d'attaques : celles par relais.

L'attaque par relais consiste, pour un pirate, à faire croire au lecteur que le tag est présent dans son champ d'interrogation alors qu'il ne l'est pas. Pour cela, le pirate, avec l'aide d'un complice, joue le rôle d'une « rallonge ». Par exemple, pour démarrer un véhicule, un pirate muni d'un ordinateur portable se situe auprès du véhicule (contenant le lecteur RFID) pendant que son complice se situe aux côtés du propriétaire du véhicule, plus précisément auprès de la personne qui détient (légitimement) la clef de démarrage (contenant le tag RFID). Le lecteur envoie un challenge, reçu par le pirate, qui le transmet à son complice. Ce challenge est envoyé à la clef de la victime qui répond correctement. Le complice transmet cette réponse au pirate qui la soumet enfin au lecteur du véhicule. La protection électronique du véhicule est ainsi outrepassée sans que le pirate ne possède la clef.

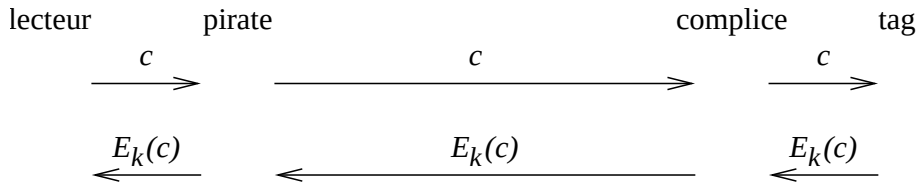

Fig. 3. Attaque par relais

Comme schématisé sur la figure 3, cette attaque est extrêmement simple, facile à mettre en œuvre et difficilement détectable par la victime. Il suffit au pirate d'être suffisamment proche de sa victime au moment même de l'attaque ; ceci peut être fait dans une file d'attente, dans le métro, etc. Bien que cette attaque soit une *man-in-the-middle attack*, on préfère la qualifier de *par relais* car le pirate dans ce cas précis ne fait que transmettre passivement les messages.

Trouver une solution purement technique à ce problème est très difficile. Les recherches actuelles (par exemple [7]) consistent à mesurer le temps de réponse du tag. Si celui-ci est trop important, l'authentification est refusée car le tag n'est probablement pas à proximité du lecteur.

3 Respect de la vie privée

Outre les problèmes directement liés à la sécurité, la RFID doit faire face aux problèmes qui touchent la vie privée. Ces problèmes concernent la divulgation d'information et la traçabilité malveillante.

3.1 Divulgation d'information

Le problème de la divulgation d'information se pose lorsque les données envoyées par le tag révèlent des informations sur l'objet qui le porte. Dans le cadre d'une bibliothèque, par exemple, l'information communiquée ouvertement peut être le titre de l'ouvrage. Plus préoccupant, les produits pharmaceutiques marqués électroniquement, comme préconisé par le *Food & Drug Administration* aux États-Unis, pourraient révéler les pathologies d'une personne : un employeur ou un assureur pourrait déterminer les médicaments détenus par une personne et en tirer des conclusions sur son état de santé. La prise en compte de cet aspect est particulièrement importante dans les applications plus évoluées où des informations personnelles sont contenues dans le transpondeur : dossier médical, passeport biométrique, etc. Aux États-Unis, l'arrivée du passeport muni d'un tag électronique, initialement prévue pour août 2005, fut différée afin de reconsidérer les aspects liées à la sécurité.

3.2 Traçabilité malveillante des individus

Les tags électroniques n'ont pas vocation à contenir ou à transmettre d'importantes quantités de données. Lorsqu'une base de données est présente dans le système, le tag peut n'envoyer qu'un simple identifiant, que seules les personnes ayant accès à la base de données peuvent relier à l'objet correspondant. C'est le principe utilisé par les systèmes à codes-barres. Cependant, même si un identifiant ne permet pas d'obtenir d'information sur l'objet lui-même, il peut permettre de le tracer, c'est-à-dire de reconnaître l'objet dans des lieux différents ou à des instants différents. On peut ainsi savoir à quelle heure une personne est passée en un lieu donné, par exemple pour déterminer son heure d'arrivée et de départ de son poste de travail, ou on peut reconstituer son chemin à partir de plusieurs lecteurs, par exemple dans une entreprise ou un centre commercial.

3.3 Défenseurs contre opposants

Du côté des promoteurs de la RFID, la thèse que les tags électroniques mettent en péril le respect de la vie privée est ardemment rejetée. Une distance de lecture réduite à quelques décimètres est le principal argument de défense. Cet argument est contesté par les opposants car, en utilisant une antenne plus performante et une puissance d'émission non réglementaire, il est possible de dépasser la limite annoncée. En outre, il existe de nombreux cas où un attaquant peut suffisamment se rapprocher de sa victime pour lire ses tags électroniques : dans les transports en commun, dans une file d'attente, etc. L'inquiétude des opposants provient également du fait que les tags sont de plus en plus présents dans la vie de tous les jours, sans qu'on le sache. Ils sont souvent invisibles, répondant aux requêtes des lecteurs à l'insu même des personnes qui les portent.

3.4 Eviter la traçabilité malveillante

Il existe des techniques pour empêcher la traçabilité malveillante et la fuite d'information. La plus radicale consiste à détruire le tag. Cette méthode ne peut être utilisée que dans des applications particulières (par exemple à la fin d'une chaîne de production) car le tag n'est ensuite plus utilisable. Il existe également des dispositifs électroniques pour bruiter l'environnement du tag, soit au niveau de la couche physique, soit au niveau de la couche communication [10] (en perturbant le protocole d'évitement de collisions utilisé par le lecteur). Les recherches se concentrent aujourd'hui sur la conception de protocoles tels qu'un lecteur autorisé puisse identifier les tags mais qu'un pirate ne soit pas en mesure de les identifier ni même de les tracer [2,3,5,9,11,12,14].

Un simple protocole par question/réponse peut suffire pour autant que l'information envoyée par le tag soit *randomizée*, comme indiqué sur la figure 4, c'est-à-dire que le tag chiffre le challenge combiné avec de l'aléa. Cela évite qu'un pirate envoyant deux fois le même challenge à un tag reçoive deux fois la même réponse, permettant ainsi de le tracer. Cependant, ce type de protocole

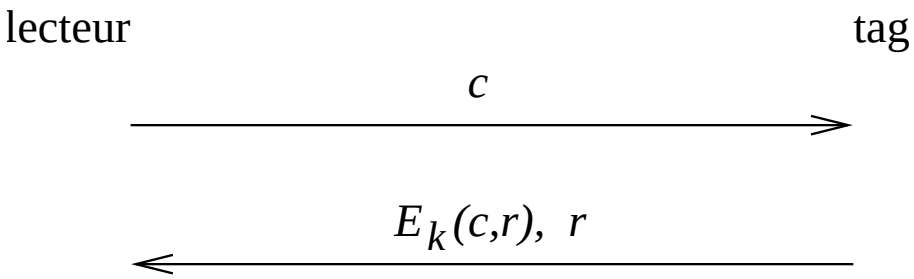

Fig. 4. Protocole par question/réponse où la réponse est randomizée

présente deux grands inconvénients :

- Il nécessite l'utilisation d'un algorithme de chiffrement et d'un générateur pseudo-aléatoire sur le tag. Cette approche n'est donc pas possible avec les tags de classe 1, ce qui nécessite l'usage de tags de classe 2, plus coûteux. Elle est donc généralement réservée aux applications nécessitant de l'authentification et non simplement de l'identification.
- Il engendre de nombreux calculs du côté du lecteur car ce dernier doit tester toutes les clefs présentes dans sa base de donnée pour déterminer l'identité du tag avec lequel il communique : pour chaque clef k, il doit calculer $E_k(c, r)$ jusqu'à trouver un résultat égal à la valeur reçue. Cette approche n'est donc possible qu'avec des systèmes RFID ne possédant que peu de tags.

Les travaux actuels cherchent donc à concevoir des algorithmes cryptographiques et des protocoles d'identification qui soient peu gourmands en ressources, afin de

pouvoir être utilisés dans des tags sans en augmenter considérablement le coût. Sous ces contraintes, les protocoles doivent rester aussi sûrs[3] que possibles.

4 Conclusion

L'identification par radiofréquence est aujourd'hui utilisée dans de nombreux domaines. Outre les aspects techniques et économiques, l'un des principaux freins à son déploiement concerne sa sécurité. Cet article s'est intéressé aux problèmes de sécurité au niveau de la communication entre le lecteur et le tag. Bien sûr, la sécurité entre le lecteur et le système de traitement des données ne doit pas être négligée, mais cet aspect n'est pas une spécificité de la RFID.

Nous avons vu que certaines applications ne sont pas directement concernées par la sécurité, alors que celle-ci constitue un élément fondamental pour certaines autres, comme le contrôle d'accès. Le choix d'un protocole RFID – et en conséquence d'un type de tag – dépend donc fortement de l'application visée. Toutefois, le problème du respect de la vie privée, en particulier celui de la traçabilité malveillante, reste entier quelque soit l'application considérée.

Enfin, les questions de sécurité ne doivent pas se borner aux protocoles cryptographiques, mais considérer la RFID dans son ensemble. Des travaux s'intéressent aujourd'hui aux couches les plus basses de la RFID pour tracer des tags, pour réaliser des dénis de service, ou encore pour exploiter des *side channel*. Récemment, un débat nouveau a vu le jour, il concerne la possibilité d'injecter des virus dans des systèmes RFID.

Références

1. Priya Agrawal, Neha Bhargava, Chaitra Chandrasekhar, Al Dahya, and J.D. Zamfirescu. The MIT ID Card System : Analysis and recommendations, December 2004.
2. Gildas Avoine. *Cryptography in Radio Frequency Identification and Fair Exchange Protocols*. PhD thesis, EPFL, Lausanne, Switzerland, December 2005.
3. Gildas Avoine, Etienne Dysli, and Philippe Oechslin. Reducing time complexity in RFID systems. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography – SAC 2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 291–306, Kingston, Canada, August 2005. Springer-Verlag.
4. Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, and Michael Szydlo. Security analysis of a cryptographically-enabled RFID device. In *USENIX Security Symposium*, pages 1–16, Baltimore, Maryland, USA, July-August 2005. USENIX.
5. Claude Castelluccia and Gildas Avoine. Noisy tags : A pretty good key exchange protocol for RFID tags. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS*, volume 3928 of *Lecture Notes in Computer Science*, pages 289–299, Tarragona, Spain, April 2006. IFIP, Springer-Verlag.

[3] La notion de *protocole sûr* en RFID est aujourd'hui encore très informelle et fait l'objet de nombreux travaux.

6. EPCGlobal. Class 1 generation 2 UHF air interface protocol standard version 1.0.9. `http://www.epcglobalinc.org`, January 2005.
7. Gerhard Hancke and Markus Kuhn. An RFID distance bounding protocol. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, Athens, Greece, September 2005. IEEE.
8. Martin Hellman. A cryptanalytic time-memory trade off. *IEEE Transactions on Information Theory*, IT-26(4) :401–406, July 1980.
9. Ari Juels. RFID security and privacy : A research survey. *IEEE Journal on Selected Areas in Communication*, 2006.
10. Ari Juels, Ronald Rivest, and Michael Szydlo. The blocker tag : Selective blocking of RFID tags for consumer privacy. In Vijay Atluri, editor, *Conference on Computer and Communications Security – CCS'03*, pages 103–111, Washington, DC, USA, October 2003. ACM, ACM Press.
11. Ari Juels and Stephen Weis. Authenticating pervasive devices with human protocols. In Victor Shoup, editor, *Advances in Cryptology – CRYPTO'05*, volume 3621 of *Lecture Notes in Computer Science*, pages 293–308, Santa Barbara, California, USA, August 2005. IACR, Springer-Verlag.
12. David Molnar and David Wagner. Privacy and security in library RFID : Issues, practices, and architectures. In Birgit Pfitzmann and Peng Liu, editors, *Conference on Computer and Communications Security – CCS'04*, pages 210–219, Washington, DC, USA, October 2004. ACM, ACM Press.
13. Philippe Oechslin. Making a faster cryptanalytic time-memory trade-off. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO'03*, volume 2729 of *Lecture Notes in Computer Science*, pages 617–630, Santa Barbara, California, USA, August 2003. IACR, Springer-Verlag.
14. Sanjay Sarma, Stephen Weis, and Daniel Engels. RFID systems and security and privacy implications. In Burton Kaliski, Çetin Kaya Koç, and Christof Paar, editors, *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 454–469, Redwood Shores, California, USA, August 2002. Springer-Verlag.